ASCAP

ASCAP
Agjencia e Sigurimit të Cilësisë së Arsimit Parauniversitar

MODUL KURRIKULAR

Kurrikula në Bazë Shkolle në Arsimin e Mesëm të Ulët

SIGURIA KIBERNETIKE

Koordinator: Eriksen Mersinllari

www.ascap.edu.al

2026

MODUL KURRIKULAR
KURRIKULA NË BAZË SHKOLLE NË ARSIMIN E MESËM TË ULËT
"SIGURIA KIBERNETIKE"

1. HYRJE

Moduli kurrikular "Siguria kibernetike" është hartuar në përputhje me parimet dhe drejtimet themelore të Kornizës Kurrikulare të Arsimit Parauniversitar dhe Kurrikulës Bërthamë për Arsimin e Mesëm të Ulët, të cilat vendosin në qendër zhvillimin e kompetencave kyçe, edukimin digjital dhe qytetar, si dhe mirëqenien e nxënësve në mjediset virtuale.

Nxënësit e klasës së gjashtë ndodhen në një fazë të rëndësishme të zhvillimit të tyre digjital. Në këtë moshë, ata fillojnë të përdorin më shpesh rrjetet sociale, aplikacionet e komunikimit, lojërat online dhe platforma të ndryshme digjitale, duke zgjeruar ndërveprimin e tyre në mjedisin virtual. Krahas mundësive të shumta që ofron teknologjia për të mësuar, komunikuar dhe bashkëpunuar, kjo moshë shoqërohet edhe me ekspozim më të madh ndaj rreziqeve konkrete, si bullizmi kibernetik, mashtrimet elektronike (phishing), cenimi i privatësisë dhe përdorimi i pasigurt i informacionit personal.

Qëllimi i modulit është të pajisë nxënësit me njohuritë, aftësitë dhe qëndrimet e nevojshme për të kuptuar, parandaluar dhe përballuar këto rreziqe, si dhe për të përdorur internetin dhe platformat digjitale në mënyrë të sigurt, të përgjegjshme dhe etike.

Në këtë kuadër, moduli synon:

- zhvillimin e të kuptuarit mbi identitetin online, gjurmën digjitale dhe ndikimin që sjellja në internet mund të ketë në jetën reale;
- identifikimin e formave kryesore të bullizmit kibernetik dhe kuptimin e pasojave emocionale, sociale dhe etike që ai mund të shkaktojë;
- formimin e shkathtësive praktike për të identifikuar, parandaluar dhe raportuar raste të bullizmit kibernetik;
- zhvillimin e aftësive për të dalluar mashtrimet elektronike (phishing), mesazhet dhe faqet e dyshimta, si dhe për të reaguar në mënyrë të sigurt ndaj tyre;
- ndërgjegjësimin për rëndësinë e mbrojtjes së të dhënave personale, privatësisë dhe përdorimit të kujdesshëm të rrjeteve sociale;
- nxitjen e përdorimit të masave bazë të mbrojtjes digjitale, si fjalëkalimet e forta, verifikimi i informacionit dhe raportimi i incidenteve;
- ndërtimin e qëndrimeve të përgjegjshme, kritike, etike dhe solidarizuese gjatë komunikimit dhe ndërveprimit në mjedisin digjital.

Moduli ka karakter praktik, ai zhvillohet kryesisht përmes veprimtarive aktive, si: skenarë për diskutim, simulime, lojëra me role, analiza rastesh dhe projekte ndërgjegjësuese, duke krijuar mundësi që nxënësit të zbatojnë në situata konkrete njohuritë e fituara. Në këtë mënyrë, moduli nuk synon thjesht përvetësimin e disa rregullave teorike, por zhvillimin e aftësisë për të menduar në mënyrë kritike, për të marrë vendime të informuara dhe për të vepruar me përgjegjësi në mjedisin digjital.

Përmes këtij moduli, nxënësit aftësohen të kuptojnë lidhjen ndërmjet jetës reale dhe asaj virtuale, të reflektojnë mbi identitetin e tyre online dhe gjurmën digjitale, të dallojnë shenjat e bullizmit kibernetik dhe mashtrimeve elektronike, si dhe të njohin mënyrat e mbrojtjes së privatësisë dhe të dhënave personale. Njëkohësisht, ata zhvillojnë gatishmërinë për të reaguar në kohë, për të kërkuar ndihmë dhe për të mbështetur të tjerët kur përballen me situata të rrezikshme në internet. Në funksion të kurrikulës me bazë kompetencat, moduli kontribuon në zhvillimin e kompetencës digjitale, të mendimit kritik, të komunikimit efektiv dhe të qytetarisë aktive. Moduli mund të zbatohet në klasën e gjashtë, në kuadër të kurrikulës me bazë shkolle, duke u përshtatur me kontekstin e shkollës, nevojat e nxënësve dhe zhvillimet bashkëkohore në fushën e teknologjisë dhe sigurisë kibernetike. Në këtë mënyrë, moduli kontribuon në formimin e nxënësve të vetëdijshëm, të përgjegjshëm dhe të përgatitur për të lundruar në mënyrë të sigurt në mjedisin digjital, duke vendosur në fokus sigurinë, privatësinë dhe mirëqenien e tyre digjitale.

2. PËRMBAJTJA E MODULIT

Moduli është strukturuar në shtatë pjesë të ndërlidhura, të cilat trajtojnë në mënyrë progresive aspekte të ndryshme të sigurisë kibernetike, duke kaluar nga të kuptuarit e identitetit dhe sjelljes në mjedisin digjital, te njohja e rreziqeve konkrete dhe mënyrat e mbrojtjes dhe reagimit ndaj tyre.

Në tematikën "***Bota digjitale dhe unë***", nxënësit njihen me konceptet bazë të identitetit online, gjurmës digjitale dhe qytetarisë digjitale. Ata reflektojnë mbi marrëdhënien ndërmjet jetës reale dhe asaj virtuale, si dhe mbi mënyrën se si sjellja e tyre në internet mund të lërë pasoja të qëndrueshme. Përmes veprimtarive të thjeshta analitike dhe reflektuese, nxënësit ndërgjegjësohen për rëndësinë e ndërtimit të një identiteti të sigurt dhe të përgjegjshëm në mjedisin digjital.

Në tematikën "***Bullizmi kibernetik***", nxënësit njihen me format kryesore të bullizmit kibernetik dhe mësojnë ta dallojnë atë nga konfliktet e zakonshme mes bashkëmoshatarëve. Trajtohen

pasojat emocionale, sociale dhe etike të kësaj dukurie, si dhe mënyrat konkrete të reagimit, si ruajtja e dëshmive, bllokimi, raportimi dhe kërkimi i ndihmës. Nëpërmjet diskutimeve, analizës së skenarëve dhe lojërave me role, nxënësit zhvillojnë empati, aftësi reagimi dhe vetëdije për rolin e tyre si viktimë, vëzhgues ose mbështetës.

Në tematikën "***Mashtrimet elektronike***" nxënësit mësojnë se çfarë është phishing dhe si funksionon si teknikë manipulimi psikologjik. Trajtohen format kryesore: email phishing, smishing (SMS), vishing (telefonik) dhe faqet e rreme, ku nxënësit mësohen të identifikojnë shenjat paralajmëruese të mesazheve dhe faqeve mashtruese. Diskutohen mënyrat e verifikimit të burimit para klikimit dhe të dhënies së informacionit personal, si dhe mbrojtja praktike nëpërmjet fjalëkalimeve të forta dhe autentikimit me dy faktorë (2FA). Nxënësit praktikojnë drejtpërdrejt duke analizuar emaile dhe faqe phishing krahasuar me origjinalin, duke simuluar vendimmarrje me skenarë SMS mashtruese dhe duke krijuar fjalëkalime të forta sipas rregullave të mësuara.

Në tematikën "***Rrjetet sociale dhe privatësia",*** nxënësit reflektojnë mbi atë çfarë ndajnë dhe çfarë duhet të mbajnë private në mjediset digjitale. Trajtohen cilësimet e privatësisë dhe mënyra e menaxhimit të tyre në platformat kryesore, si dhe pasojat afatgjata të ndarjes së informacionit personal. Nxënësit njihen me të drejtat e fëmijëve në mjediset digjitale dhe ushtrohen praktikisht duke kategorizuar lloje të ndryshme informacioni dhe duke audituar një profil imagjinar, me qëllim identifikimin e problemeve të privatësisë dhe propozimin e ndryshimeve konkrete.

Në tematikën "***Reagimi, raportimi dhe ndihma"***, nxënësit njihen me mënyrat dhe kanalet e raportimit të incidenteve në mjedisin digjital, si në nivel shkolle, familjeje dhe platformash online, ashtu edhe në nivel institucional. Kjo pjesë i ndihmon ata të kuptojnë se reagimi i shpejtë dhe kërkimi i ndihmës janë pjesë thelbësore e mbrojtjes në mjedisin online. Përmes veprimtarive praktike dhe ushtrimeve të strukturuara, nxënësit organizojnë dhe përforcojnë njohuritë e marra gjatë modulit.

Në pjesën "***Përgatitja për produktin final***", nxënësit punojnë në grupe për të planifikuar, organizuar dhe strukturuar materialet që do të përdorin në produktin përmbyllës të modulit. Ata ndajnë role, përcaktojnë detyrat dhe përzgjedhin formatin më të përshtatshëm për prezantimin e mesazheve ndërgjegjësuese. Faza përmbyllëse e modulit është organizimi dhe prezantimi i fushatës ndërgjegjësuese në nivel shkolle, ku nxënësit zbatojnë të gjitha njohuritë dhe aftësitë e fituara gjatë modulit. Çdo grup prezanton materialin e vet: poster, broshurë, video ose kuiz, përpara një audience që mund të përfshijë nxënës të klasave të tjera, mësues dhe prindër. Pas

prezantimit zhvillohet një reflektim i hapur mbi përvojën e të nxënit, duke nxjerrë mësime mbi rëndësinë e sigurisë kibernetike, mendimit kritik dhe solidaritetit digjital në jetën e përditshme.

Përmbajtja e modulit krijon mundësi për integrim ndërkurrikular me lëndë dhe fusha të ndryshme të të nxënit:

- *Teknologjia e Informacionit dhe Komunikimit (TIK):* kuptimi i rreziqeve në mjedisin digjital, njohja me format e mashtrimeve elektronike, mbrojtja e të dhënave personale dhe përdorimi i masave bazë të sigurisë digjitale;
- *Qytetaria:* zhvillimi i përgjegjësisë, respektit dhe sjelljes etike në mjedisin online, si dhe ndërgjegjësimi për të drejtat dhe detyrimet e qytetarit digjital;
- *Gjuha shqipe:* analizimi i mesazheve dhe përmbajtjeve digjitale, argumentimi i qëndrimeve, zhvillimi i komunikimit të qartë dhe ndërtimi i mesazheve ndërgjegjësuese;
- *Arte*: realizimi i posterave, broshurave, infografikëve dhe materialeve të tjera vizuale me mesazhe ndërgjegjësuese për sigurinë kibernetike;
- *Shkencat shoqërore:* kuptimi i pasojave sociale dhe etike të bullizmit kibernetik, mashtrimeve elektronike dhe cenimit të privatësisë në mjedisin digjital.

3. KLASA/T KU MUND TË ZHVILLOHET MODULI

Moduli është parashikuar të zhvillohet me nxënës të klasës së gjashtë. Ai ofron fleksibilitet në përshtatjen e kohëzgjatjes dhe thellësisë së përmbajtjes, duke mundësuar që të jetë në përputhje me moshën e nxënësve, nivelin e të kuptuarit dhe zhvillimin e kompetencave të tyre. Gjithsesi shkollat kamë fleksibilitet të përzgjedhin klasën më të përshtatshme për zbatimin e modulit, duke marrë parasysh nevojat, interesat e nxënësve dhe kontekstin pedagogjik të institucionit.

4. MËSUESIT QË MUND TË ZHVILLOJNË MODULIN

Moduli rekomandohet të zhvillohet kryesisht nga mësuesit e Teknologjisë së Informacionit dhe Komunikimit (TIK), mësuesit e qytetarisë, si dhe nga mësuesit e arsimit fillor, pasi përmbajtja dhe tematika e tij lidhen drejtpërdrejt me zhvillimin e kompetencës digjitale, edukimin qytetar dhe formimin e sjelljeve të sigurta dhe të përgjegjshme tek nxënësit.

Megjithatë, shkolla ka fleksibilitet në përcaktimin e mësuesve që do ta zhvillojnë modulin, në varësi të kontekstit institucional, strukturës së stafit dhe zhvillimit profesional të tij. Në këtë kuadër, moduli mund të realizohet edhe nga mësues të tjerë të formimit ndërdisiplinor, të cilët kanë kompetencat pedagogjike dhe përgatitjen e nevojshme për të udhëhequr veprimtaritë e parashikuara. Ky fleksibilitet siguron që moduli të mos kufizohet vetëm te një fushë mësimore,

por të përfitojë nga ekspertiza dhe përvoja e mësuesve në funksion të rritjes së cilësisë së procesit mësimor dhe zhvillimit të kompetencave të nxënësve.

Pavarësisht profilit, mësuesi që zhvillon modulin duhet të njohë platformat kryesore digjitale që përdorin nxënësit e kësaj moshe dhe të jetë i aftë të menaxhojë diskutime të ndjeshme si bullizmi kibernetik me empati dhe profesionalizëm. Rekomandohet bashkëpunim ndërdisiplinor, sidomos gjatë organizimit të produktit final.

Rekomandime për mësuesit

Gjatë zhvillimit të modulit:

- Krijoni një mjedis të sigurt dhe mbështetës, ku nxënësit të ndihen të lirshëm për të ndarë përvoja, shqetësime dhe pyetje që lidhen me përdorimin e internetit, rrjeteve sociale dhe teknologjisë.
- Përdorni gjuhë të qartë, konkrete dhe të përshtatshme për moshën e nxënësve, duke shpjeguar termat teknikë me shembuj nga jeta e përditshme.
- Fokusohuni te zhvillimi i të menduarit kritik dhe i aftësive praktike, jo vetëm te përvetësimi i informacionit teorik.
- Përdorni situata reale ose të ngjashme me përvojat e nxënësve për të trajtuar tema si bullizmi kibernetik, mashtrimet elektronike, privatësia dhe përdorimi i rrjeteve sociale.
- Inkurajoni diskutime të hapura, reflektim dhe analizë të rasteve, duke i ndihmuar nxënësit të kuptojnë pasojat e sjelljeve në mjedisin digjital.
- Theksoni gjithmonë zgjidhjet praktike, mënyrat e mbrojtjes dhe hapat e reagimit në situata të pasigurta.

Menaxhimi i situatave të ndjeshme

- Tregoni kujdes dhe ndjeshmëri ndaj nxënësve që mund të kenë përjetuar situata të bullizmit kibernetik, cenimit të privatësisë ose përvoja të tjera shqetësuese në mjedisin online.
- Inkurajoni nxënësit të raportojnë dhe të kërkojnë ndihmë nga një i rritur i besuar, kur përballen me përmbajtje, komunikime ose situata që i shqetësojnë.
- Përdorni një qasje mbështetëse dhe inkurajuese, duke nxitur empatinë, respektin dhe solidaritetin digjital ndërmjet nxënësve.
- Në rastet kur evidentohen shqetësime konkrete, bashkëpunoni me psikologun e shkollës, prindërit dhe strukturat përkatëse mbështetëse.

Përshtatja e modulit

- Përshtatini veprimtaritë sipas nivelit të zhvillimit, përvojave digjitale dhe nevojave të nxënësve të klasës.

- Zgjeroni ose thjeshtoni trajtimin e çështjeve të caktuara në varësi të njohurive paraprake dhe interesit të nxënësve.
- Përzgjidhni ose modifikoni skenarët, rastet studimore dhe simulimet sipas kontekstit të shkollës dhe realitetit të nxënësve.
- Shtoni shembuj dhe platforma që nxënësit përdorin realisht, në mënyrë që përmbajtja të jetë më e afërt dhe më kuptimplote për ta.
- Mund të planifikoni, sipas mundësive dhe në bashkëpunim me drejtuesit e shkollës, përfshirjen e ekspertëve nga fusha e sigurisë kibernetike, psikologjisë shkollore ose institucioneve mbështetëse, të cilët mund të kontribuojnë me njohuri dhe përvoja praktike.

5. KOHËZGJATJA E MODULIT

Moduli mund të integrohet në kurrikulën me bazë shkolle si një program i plotë prej **35 orësh** mësimore. Ai mund të zbatohet duke përfshirë veprimtaritë e sugjeruara për secilën tematikë, si dhe veprimtari të tjera që mësuesi i vlerëson të përshtatshme, në përputhje me nevojat dhe kontekstin e nxënësve.

Tematika/Përmbajtja	Orë mësimore	% e kohës
1. Bota digjitale dhe unë	4	11%
2. Bullizmi kibernetik	8	23%
3. Mashtrimet elektronike (Phishing)	8	23%
4. Rrjetet sociale dhe privatësia	4	11%
5. Reagimi, raportimi dhe ndihma	4	11%
6. Përgatitja për produktin final	3	9%
7. Produkti final: Fushata e ndërgjegjësimit	4	12%
TOTAL	**35**	**100%**

6. REZULTATET E TË NXËNIT

Rezultatet e të nxënit
Tematika: Bota digjitale dhe unë
Nxënësi: • përshkruan identitetin online dhe gjurmën digjitale përmes shembujve konkretë; • dallon sjelljet e përshtatshme dhe të papërshtatshme në mjediset virtuale;

- shpjegon lidhjen ndërmjet sjelljes në jetën reale dhe asaj në botën digjitale;
- vlerëson rëndësinë e qytetarisë digjitale si pjesë e jetës së përditshme.

Tematika: Ndjenjat dhe përjetimet në mjedisin online

Nxënësi:

- përkufizon bullizmin kibernetik dhe e dallon atë nga konfliktet e zakonshme mes bashkëmoshatarëve;
- identifikon format kryesore të bullizmit kibernetik, si fyerja, imitimi, përjashtimi dhe kërcënimi;
- analizon pasojat emocionale, sociale dhe etike të bullizmit kibernetik për viktimën, autorin dhe vëzhguesin;
- zbaton hapat praktikë të reagimit ndaj bullizmit kibernetik, si raportimi, bllokimi, ruajtja e dëshmive dhe kërkimi i ndihmës;
- vlerëson rolin e vëzhguesit dhe mënyrat se si ai mund të mbështesë viktimën;
- zhvillon qëndrime etike, empatike dhe të përgjegjshme ndaj bashkëmoshatarëve në mjediset online.

Tematika: Mashtrimet elektronike

Nxënësi:

- shpjegon konceptin e phishing dhe mënyrën se si ai funksionon si formë mashtrimi në mjedisin digjital;
- identifikon format kryesore të phishing, si email phishing, smishing (SMS), vishing (telefonik) dhe faqet e rreme;
- dallon shenjat paralajmëruese të mesazheve, lidhjeve dhe faqeve mashtruese;
- zbaton strategji të thjeshta verifikimi përpara klikimit të lidhjeve ose dhënies së të dhënave personale;
- përdor masa bazë mbrojtëse, si krijimi i fjalëkalimeve të forta dhe autentikimi me dy faktorë (2FA);
- analizon raste dhe situata të simuluara phishing, duke argumentuar reagimin e duhur.

Tematika: Rrjetet sociale dhe privatësia

Nxënësi:

- dallon llojet e informacionit që mund të ndahet dhe ato që nuk duhet të publikohen në mjedisin online;
- zbaton cilësimet bazë të privatësisë në platformat dhe rrjetet sociale më të përdorura;
- analizon pasojat që mund të sjellë ndarja e pakujdesshme e informacionit personal;

• shpjegon rëndësinë e mbrojtjes së privatësisë dhe të të dhënave personale në mjedisin digjital; • njeh të drejtat e fëmijëve në mjediset digjitale dhe rëndësinë e respektimit të tyre.
Tematika: Unë veproj
Nxënësi: • zbaton hapat e raportimit të incidenteve kibernetike në platforma, në shkollë dhe në familje; • identifikon burimet institucionale të ndihmës dhe mbështetjes në nivel kombëtar. • përdor mënyra të përshtatshme reagimi në situata që cenojnë sigurinë dhe privatësinë në internet; • reflekton mbi njohuritë e fituara gjatë modulit dhe identifikon fushat që kërkojnë rishikim ose përforcim.
Produkti final: Fushata e ndërgjegjësimit
Nxënësi: • prezanton fushatën ndërgjegjësuese para bashkëmoshatarëve dhe komunitetit shkollor; • zbaton në mënyrë të integruar njohuritë, aftësitë dhe qëndrimet e zhvilluara gjatë modulit në një produkt konkret; • komunikon mesazhe të qarta dhe të përshtatshme për sigurinë kibernetike dhe përdorimin e përgjegjshëm të teknologjisë; • reflekton mbi përvojën e të nxënit dhe nxjerr përfundime mbi rëndësinë e sigurisë, privatësisë dhe mirëqenies digjitale.

7. VEPRIMTARITË PRAKTIKE

Në vazhdim janë përshkruar veprimtari praktike të sugjeruara, të grupuara sipas tematikave të modulit. Mësuesi është i lirë të përzgjedhë midis veprimtarive të sugjeruara në modul, t'i përshtatë ato si dhe plotësojë me veprimtari të tjera të cilat e mbështesin për të trajtuar tematikat dhe për të përmbushur rezultatet e të nxënit.

BOTA DIGJITALE DHE UNË

✓ ***Çështjet kryesore që trajtohen:***

- Çfarë është identiteti online dhe gjurma digjitale?
- Si ndërveprojmë ndryshe online dhe offline?
- Çfarë nënkupton të qenurit "*qytetar digjital i përgjegjshëm*"?

- Lidhja midis botës reale dhe asaj virtuale — ngjashmëritë dhe rreziqet.

Veprimtari: Kush jam unë online?

***Qëllimi i veprimtarisë*:** Nxënësit reflektojnë mbi identitetin e tyre online dhe krahasojnë mënyrën si paraqiten në mjedisin digjital me mënyrën si janë në jetën reale.

***Përshkrimi i veprimtarisë*:** Veprimtaria nis me një bisedë hyrëse, ku mësuesi i fton nxënësit të reflektojnë mbi pyetjen: *"Nëse dikush nuk ju njeh fare, çfarë mund të mësojë për ju vetëm duke parë profilin ose praninë tuaj online?"* Nxënësit ndajnë mendime dhe mësuesi shkruan në tabelë fjalë kyçe që lidhen me mënyrën si paraqitemi në internet, si p.sh. foto, komente, pëlqime, postime, interesa, mënyra e komunikimit.

Më pas, nxënësit punojnë individualisht dhe ndërtojnë dy profile paralele: *"Unë online"* dhe **"***Unë në jetën reale***"**. Ata mund t'i paraqesin këto në formë tabele, skeme, vizatimi ose përshkrimi me pika. Mësuesi i udhëzon të reflektojnë mbi pyetje të tilla si:

- Çfarë tregoj për veten online?
- Çfarë zgjedh të mos tregoj?
- A ka gjëra që i ekzagjeroj ose i paraqes ndryshe?
- A jam i njëjti person online dhe në jetën reale?

Në vijim zhvillohet një diskutim i hapur në klasë, ku nxënësit, me dëshirë, ndajnë vëzhgimet e tyre. Mësuesi udhëheq reflektimin mbi çështje si:

- Pse ndonjëherë njerëzit sillen ndryshe online?
- Çfarë pasoja mund të ketë kjo për ta dhe për të tjerët?
- Pse është e rëndësishme të jemi të përgjegjshëm edhe në mjedisin digjital?

Në përfundim, mësuesi thekson se identiteti online është pjesë e identitetit tonë dhe se mënyra si paraqitemi dhe komunikojmë në internet ndikon në mënyrën si na perceptojnë të tjerët.

***Produkti i mundshëm*:** Dy profile të krahasuara ("Unë online" dhe "Unë në jetën reale") dhe një reflektim i shkurtër individual mbi ngjashmëritë dhe dallimet.

Veprimtari: Gjurma ime digjitale

***Qëllimi i veprimtarisë*:** Nxënësit kuptojnë konceptin e gjurmës digjitale dhe ndërgjegjësohen për faktin se çdo veprim në internet lë pas informacion që mund të ketë ndikim në të tashmen dhe në të ardhmen.

***Përshkrimi i veprimtarisë*:** Mësuesi e nis veprimtarinë me një prezantim të shkurtër, ku shpjegon se çdo veprim që kryejmë në internet lë gjurmë digjitale. Ai sjell shembuj konkretë,

si: kërkimet në internet, komentet, pëlqimet, fotografitë e postuara, aplikacionet e përdorura, lojërat online apo mesazhet e dërguara.

Pas këtij shpjegimi, nxënësit ftohen të reflektojnë individualisht mbi aktivitetet e tyre online gjatë javës së fundit. Ata mund të listojnë, në mënyrë të përgjithshme dhe pa hyrë në të dhëna personale, veprime si:

- çfarë kanë kërkuar;
- çfarë kanë parë ose shpërndarë;
- me kë kanë komunikuar;
- çfarë aplikacionesh ose lojërash kanë përdorur.

Më pas, nxënësit ndahen në grupe dhe ndërtojnë një **hartë të gjurmës digjitale**, ku paraqesin në mënyrë vizuale se si dhe ku lëvizin të dhënat në internet: motorë kërkimi, rrjete sociale, aplikacione, faqe interneti, lojëra online etj. Mësuesi i ndihmon të kuptojnë se këto të dhëna mund të ruhen, të analizohen dhe të përdoren nga platformat digjitale.

Në vijim, zhvillohet një diskutim i drejtuar me pyetje si:

- Cilat gjurmë digjitale janë të padëmshme dhe cilat mund të bëhen problem?
- Çfarë pasoje mund të ketë një postim ose koment pas disa vitesh?
- Si mund të jemi më të kujdesshëm me atë që lëmë pas në internet?

Në përfundim, nxënësit përmbledhin disa vendime konkrete që mund të marrin për të reduktuar gjurmët e panevojshme dhe për të përdorur internetin në mënyrë më të përgjegjshme.

***Produkti i mundshëm*:** Hartë vizuale e gjurmës digjitale në grup dhe një listë individuale me 3 vendime konkrete për përdorim më të kujdesshëm të internetit.

Veprimtari: Çfarë lë pas në internet?

Qëllimi i veprimtarisë: Nxënësit kuptojnë se çdo veprim i kryer në internet lë gjurmë digjitale dhe reflektojnë mbi pasojat që këto gjurmë mund të kenë në të tashmen dhe në të ardhmen.

Përshkrimi i veprimtarisë: Veprimtaria nis me një bisedë hyrëse, ku mësuesi i fton nxënësit të reflektojnë mbi pyetjen: *"A zhduket gjithmonë ajo që postojmë në internet, apo diçka mbetet pas?"* Nxënësit japin mendime dhe shembuj nga përvoja e tyre. Mësuesi i orienton drejt idesë se kërkimet, komentet, postimet, pëlqimet, fotografitë, shkarkimet apo regjistrimet në faqe të ndryshme lënë gjurmë digjitale.

Më pas, mësuesi paraqet disa situata të thjeshta, si p.sh.:

- kërkimi i një informacioni në internet;
- regjistrimi në një lojë apo aplikacion;

- vendosja e një “pëlqimi” ose komenti;
- ngarkimi i një fotografie;
- shkarkimi i një aplikacioni.

Nxënësit punojnë në grupe të vogla dhe diskutojnë për secilën situatë:

- Çfarë gjurme lë kjo veprimtari?
- Kush mund ta shohë ose ta ruajë këtë informacion?
- A mund të mbetet kjo gjurmë edhe më vonë?
- Çfarë duhet të kemi parasysh përpara se ta kryejmë këtë veprim?

Në vijim, grupet paraqesin përfundimet e tyre dhe mësuesi i ndihmon të kuptojnë se gjurma digjitale nuk lidhet vetëm me atë që publikojmë, por edhe me atë që kërkojmë, klikojmë apo përdorim në mjedisin online. Theksohet se disa gjurmë mund të jenë të padëmshme, por të tjera mund të ndikojnë në privatësinë, sigurinë apo imazhin tonë në të ardhmen.

Në përfundim, nxënësit hartojnë një listë të shkurtër me rregulla orientuese për të qenë më të kujdesshëm me gjurmën e tyre digjitale, si p.sh.:

- mendoj para se të postoj;
- kontrolloj para se të regjistrohem;
- nuk jap informacion të panevojshëm;
- kujdesem për atë që lë pas në internet.

Produkti i mundshëm: Poster ose listë me rregulla të thjeshta për kujdesin ndaj gjurmës digjitale.

BULLIZMI KIBERNETIK

✓ **Çështjet kryesore që trajtohen:**

- Çfarë është bullizmi kibernetik dhe format kryesore
- Pasojat emocionale, sociale dhe juridike
- Si të reagoj si viktimë ose vëzhgues
- Raportimi, bllokimi dhe kërkimi i ndihmës
- Ndërtimi i empatie dhe kulturës kundër ngacmimit

Veprimtari: Bullizëm kibernetik apo keqkuptim?

***Qëllimi i veprimtarisë*:** Nxënësit dallojnë bullizmin kibernetik nga konfliktet e zakonshme mes bashkëmoshatarëve dhe identifikojnë format kryesore në të cilat ai shfaqet.

***Përshkrimi i veprimtarisë*:** Veprimtaria nis me një prezantim të shkurtër nga mësuesi, i cili shpjegon se jo çdo konflikt apo shaka në internet përbën bullizëm kibernetik. Në vijim, ai

prezanton tre elemente kryesore që ndihmojnë në dallimin e bullizmit kibernetik: qëllimi për të dëmtuar, përsëritja e sjelljes në kohë dhe pabarazia e fuqisë ndërmjet personave të përfshirë. Mësuesi shpjegon edhe disa forma të zakonshme të bullizmit kibernetik, si fyerja, përjashtimi, imitimi, kërcënimi dhe shpërndarja e materialeve pa leje.

Më pas, nxënësit ndahen në grupe të vogla dhe marrin kartela me skenarë të ndryshëm. Çdo grup diskuton secilin rast dhe vendos nëse bëhet fjalë për bullizëm kibernetik apo për një keqkuptim/konflikt të zakonshëm. Nxënësit argumentojnë zgjedhjen e tyre duke iu referuar kritereve të mësuara.

Skenarë për diskutim: Mësuesi shpërndan kartela me skenarë. Grupet diskutojnë dhe kategorizojnë sipas tabelës:

Skenari	**Bullizmi kibernetik?**	**Argumenti**
Erisi i dërgon vazhdimisht Anës mesazhe fyese dhe tallëse në rrjet social, pasi ajo nuk pranoi ta shtojë si mik.	Po	Qëllim dëmtimi + përsëritje
Dy shokë shkëmbejnë mesazhe me shaka mes tyre dhe të dy e përjetojnë situatën si argëtuese, pa u ndier të lënduar.	Jo	Mungon qëllimi i dëmtimit
Dikush publikon pa leje fotografinë e një nxënësi dhe nxënës të tjerë fillojnë të bëjnë komente tallëse nën postim.		
Një nxënës krijon një profil të rremë me emrin dhe fotografinë e shokut të tij, me qëllim që ta turpërojë para të tjerëve.		
Një grup nxënësish e përjashton me qëllim një bashkëmoshatar nga biseda e grupit dhe i dërgon mesazhe të ftohta ose përçmuese kur ai përpiqet të rikthehet.		

Në vijim, grupet prezantojnë përfundimet e tyre para klasës. Mësuesi udhëheq diskutimin, sqaron rastet më të paqarta dhe ndihmon nxënësit të kuptojnë se jo vetëm veprimi, por edhe qëllimi, mënyra dhe ndikimi i tij kanë rëndësi në vlerësimin e situatës. Në përfundim, mësuesi përmbledh idetë kryesore dhe thekson se të dallosh në kohë bullizmin kibernetik është hapi i parë për ta ndalur atë.

Produkti i mundshëm: Tabelë e plotësuar me skenarët, kategorizimin dhe argumentimin përkatës.

Veprimtari: Çfarë ndjen viktima?

***Qëllimi i veprimtarisë*:** Nxënësit kuptojnë pasojat emocionale dhe sociale të bullizmit kibernetik dhe zhvillojnë empati ndaj viktimave.

***Përshkrimi i veprimtarisë*:** Mësuesi përgatit 3-4 skenarë të shkurtër me role të ndryshme: viktima, autori, vëzhgues pasiv, vëzhgues që ndërhyn, prind/mësues. Nxënësit ndahen në grupe dhe luajnë skenarët me role të rrotulluara.

Skenar shembull — "Imazhi i papërshtatshëm": Klara gjen se dikush ka postuar në grupin e klasës një foto të saj të nxjerrë jashtë kontekstit me komente tallëse.

Grupi diskuton: Si ndihet Klara? Çfarë bëjnë vëzhguesit? Çfarë duhet të bëjë Klara? Çfarë mund të bënte kushdo për ta ndalur?

Reflektim pas secilës skenë: Mësuesi udhëheq diskutim me pyetje: "Si ndihesha në këtë rol? Çfarë ishte më e vështirë? Çfarë do të bëja ndryshe? Pse vëzhguesit shpesh nuk ndërhyjnë dhe çfarë ndryshon kur dikush vepron?"

Shënim metodologjik për mësuesin: Ky aktivitet mund të ngjallë emocione të forta nëse nxënës kanë eksperiencë personale me bullizmin kibernetik. Mësuesi duhet të krijojë hapësirë të sigurt, të mos detyrojë asnjë nxënës të luajë rol dhe të ketë plan mbështetjeje nëse nxënës tregon shqetësim personal.

Produkti: Fletë reflektimi individuale: "Tri gjëra që mësova sot dhe një gjë që do të bëj ndryshe si vëzhgues."

Veprimtari: Si të reagoj kur përballem me bullizëm kibernetik?

Qëllimi i veprimtarisë: Nxënësit njohin dhe zbatojnë hapat praktikë të reagimit ndaj bullizmit kibernetik.

***Përshkrimi i veprimtarisë*:** Veprimtaria nis me një diskutim të shkurtër, ku mësuesi pyet nxënësit se çfarë mund të bëjë një person kur përballet me bullizëm kibernetik. Më pas, mësuesi prezanton pesë hapa bazë reagimi:

- MOS U PËRGJIGJ me të njëjtën mënyrë — kjo i jep më shumë fuqi autorit;
- RUAJ DËSHMINË — screenshot me datë dhe orë, ruaje në vend të sigurt;
- BLOKO dhe RAPORTO llogarinë drejtpërdrejt në platformë;
- TREGOJI një të rrituri të besuar — prind, mësues, psikolog shkolle;

- KËRKO NDIHMË PROFESIONALE nëse ndjen pasoja emocionale..

Në vijim, nxënësit punojnë në grupe dhe analizojnë situata konkrete për të vendosur se cilët hapa duhet të ndërmerren dhe në çfarë rendi. Mësuesi mund të përdorë edhe ilustrime ose udhëzime vizuale për të treguar si funksionon raportimi ose bllokimi në platforma të ndryshme. Pas diskutimit, grupet prezantojnë përgjigjet e tyre dhe klasa ndërton së bashku një përmbledhje të hapave kryesorë. Mësuesi thekson se reagimi i shpejtë dhe kërkimi i ndihmës janë veprime mbrojtëse dhe jo shenjë dobësie.

***Produkti i mundshëm*:** Poster ose skemë me titullin: **"5** hapat që ndjek kur përballem me bullizëm kibernetik."

Veprimtari: Të drejtat e mia dhe kufijtë e mi në mjedisin digjital

Qëllimi i veprimtarisë: Nxënësit kuptojnë se bullizmi kibernetik cenon të drejtat dhe dinjitetin e individit dhe reflektojnë mbi përgjegjësitë që kanë në mjedisin digjital.

Përshkrimi i veprimtarisë: Mësuesi nis veprimtarinë me një shpjegim të thjeshtuar, duke theksuar se bullizmi kibernetik nuk është vetëm një sjellje e papërshtatshme, por mund të shkelë edhe të drejta themelore, si privatësia, dinjiteti dhe e drejta e imazhit. Pa hyrë në implikime juridike, ai i ndihmon nxënësit të kuptojnë se veprimet në internet kanë pasoja reale dhe se secili ka jo vetëm liri, por edhe përgjegjësi.

Në vijim, nxënësit ndahen në grupe dhe diskutojnë pyetje si:

- Ku mbaron liria ime e shprehjes dhe ku fillon dëmtimi i tjetrit?
- Pse një koment ose postim në internet mund të jetë më i dëmshëm sesa një fjalë e thënë në moment?
- Pse duhet të respektojmë privatësinë dhe imazhin e të tjerëve?

Pas diskutimit, secili grup harton një listë të shkurtër me të drejta dhe kufij që duhen respektuar në mjedisin digjital. Grupet prezantojnë punën e tyre dhe mësuesi përmbledh idetë kryesore.

Në përfundim, theksohet se përdorimi i internetit kërkon jo vetëm njohuri teknike, por edhe etikë, respekt dhe vetëkontroll.

Produkti i mundshëm: "E drejta ime dhe kufiri i saj" 5 të drejta që kam si nxënës online dhe 5 kufij që duhet të respektoj ndaj të tjerëve.

MASHTRIMET ELEKTRONIKE

✓ **Çështjet kryesore që trajtohen:**

- Kuptimi i phishing-ut si formë mashtrimi në mjedisin digjital;

- Format kryesore të phishing-ut: email, mesazhe sms, telefonata mashtruese dhe faqe të rreme;
- Dallimi i shenjave paralajmëruese të mesazheve dhe faqeve mashtruese;
- Masat praktike të mbrojtjes, si verifikimi i burimit, përdorimi i fjalëkalimeve të forta dhe autentikimi me dy faktorë (2fa);
- Mënyrat e reagimit në rastet kur një përdorues përballet me tentativa mashtrimi ose është mashtruar.

Veprimtari: Ky email duket i dyshimtë!

Qëllimi i veprimtarisë: Nxënësit dallojnë shenjat paralajmëruese të email-eve mashtruese dhe ushtrohen në identifikimin e rasteve të phishing-ut.

***Përshkrimi i veprimtarisë*:** Veprimtaria nis me një prezantim krahasimor, ku mësuesi paraqet me projektor dy email-e: një autentik dhe një phishing, pa treguar paraprakisht se cili është i rremë. Nxënësit vëzhgojnë dhe përpiqen të identifikojnë ndryshimet ndërmjet tyre.

Mësuesi prezanton dhe diskuton shenjat paralajmëruese:

- Adresa e dërguesit e dyshimtë (p.sh. support@bank-alerte-secure.com)
- Gjuhë urgjente dhe kërcënuese: "Llogaria juaj do bllokohet brenda 24 orësh!"
- Lidhje (link) që nuk përputhet me tekstin kur e vendosim miun mbi të
- Kërkesa për fjalëkalim, PIN, kod verifikimi ose të dhëna të kartës
- Gabime drejtshkrimore, gramatikore ose stil jo-profesional
- Oferta shumë tërheqëse dhe të pamundshme: "Ke fituar 1000 euro!"

Në vijim, nxënësit ndahen në grupe dhe secili grup merr 3–4 email-e të shtypura ose të simuluara. Detyra e tyre është t'i analizojnë dhe të plotësojnë një tabelë ku identifikojnë shenjat e phishing-ut, vendosin nëse email-i është real apo mashtrues dhe japin argumentin kryesor për zgjedhjen e tyre. Në fund, grupet prezantojnë analizën para klasës. Mësuesi sqaron pikat kryesore dhe ndihmon nxënësit të përforcojnë kriteret që duhet të ndjekin për të dalluar email-et e dyshimta.

***Produkti i mundshëm*:** Tabelë e plotësuar e analizës së email-eve dhe një checklistë personale me pikat kryesore që nxënësi duhet të kontrollojë përpara se të klikojë një lidhje ose të përgjigjet ndaj një email-i.

Email-i	Shenjat e phishing-ut	Phishing / Real?	Argumenti kryesor
Email 1			
Email 2			

Email 3			
Email 4			

Veprimtari: Faqja e rreme, dalloj faqet phishing

***Qëllimi i veprimtarisë*:** Nxënësit mësojnë të dallojnë një faqe të rreme nga një faqe zyrtare, duke u mbështetur te shenjat kryesore të sigurisë dhe besueshmërisë.

***Përshkrimi i veprimtarisë*:** Veprimtaria nis me një prezantim vizual krahasimor, ku mësuesi shfaq një faqe zyrtare dhe një kopje phishing të së njëjtës faqe ose të një institucioni të ngjashëm. Nxënësit vëzhgojnë me kujdes dhe identifikojnë dallimet, si:

- URL e ndryshme;
- logo jo plotësisht identike;
- mungesa e HTTPS ose certifikatës së sigurisë;
- gabime vizuale;
- formulim jo profesional i tekstit.

Më pas, mësuesi zhvillon ushtrimin praktik "Kliko apo jo?", ku u paraqet nxënësve disa URL të shtypura ose në ekran. Secili nxënës vendos nëse do të klikonte ose jo dhe argumenton vendimin e tij. Pas përgjigjeve, zhvillohet një diskutim i shkurtër mbi rastet ku nxënësit kanë mendime të ndryshme. Mësuesi thekson rregullin bazë se nuk duhen ndarë fjalëkalime, kode apo të dhëna personale pas klikimit të një lidhjeje të ardhur me email ose SMS, por duhet hyrë gjithmonë drejtpërdrejt në faqen zyrtare duke shkruar vetë adresën.

Produkti i mundshëm: Listë personale me titull: "5 *gjëra që kontrolloj para se të klikoj."*

Veprimtari: Ku klikova gabim?

***Qëllimi i veprimtarisë*:** Nxënësit analizojnë një situatë të simuluar mashtrimi elektronik dhe kuptojnë pasojat që mund të sjellë një klikim i pakujdesshëm.

***Përshkrimi i veprimtarisë*:** Mësuesi paraqet një skenar të thjeshtë, si p.sh.: një mesazh SMS ku njoftohet fitimi i një çmimi dhe kërkohet klikimi i një lidhjeje dhe dhënia e informacionit personal. Nxënësit diskutojnë fillimisht se si do të reagonin në një situatë të tillë. Mësuesi i ndihmon të identifikojnë një nga një elementet që e bëjnë këtë mesazh të dyshimtë. Më pas, diskutimi zhvendoset te pyetja: "Çfarë mund të ndodhë nëse klikoj?"

Në vijim, mësuesi shpjegon zinxhirin e mundshëm të pasojave, si vjedhja e të dhënave, aksesi në kontakte, shpërndarja e mesazheve mashtruese te të tjerët ose instalimi i programeve të dëmshme.

Si pjesë e veprimtarisë, mund të zhvillohet një mini-debat në klasë, ku një grup nxënësish përpiqet të shpjegojë pse mesazhi mund të duket bindës, ndërsa grupi tjetër argumenton pse ai është i dyshimtë dhe si duhet reaguar. Në këtë mënyrë, nxënësit jo vetëm identifikojnë rrezikun, por edhe kuptojnë mekanizmat e manipulimit.

***Produkti i mundshëm*:** Diagram rrjedhe me titull: *"Çfarë ndodh nëse klikoj?"*, ku paraqiten hapat dhe pasojat e një veprimi të pakujdesshëm.

Veprimtari: Fjalëkalimi i fortë dhe 2FA

***Qëllimi i veprimtarisë*:** Nxënësit kuptojnë rëndësinë e përdorimit të fjalëkalimeve të forta dhe të autentikimit me dy faktorë si masa bazë mbrojtjeje në mjedisin digjital.

***Përshkrimi i veprimtarisë*:** Veprimtaria nis me një prezantim interaktiv, ku mësuesi shpjegon rregullat bazë të krijimit të një fjalëkalimi të fortë. Diskutohet me nxënësit pse fjalëkalimet e dobëta janë një nga shkaqet kryesore që lejojnë aksesin e paautorizuar në llogari. Mësuesi paraqet kriteret kryesore të një fjalëkalimi të sigurt, si gjatësia, kombinimi i shkronjave, numrave dhe simboleve, shmangia e të dhënave personale dhe përdorimi i fjalëkalimeve të ndryshme për llogari të ndryshme. Në vijim, nxënësit analizojnë disa shembuj fjalëkalimesh dhe i klasifikojnë si të dobëta, të pranueshme ose të forta, duke argumentuar vlerësimin e tyre. Diskutimi ndihmon në kuptimin e tipareve që e bëjnë një fjalëkalim më të sigurt.

Fjalëkalimi	Vlerësimi	Arsyeja
123456	Shumë i dobët	Sekuencë e zakonshme, e para në çdo sulm brute-force
Erjon2010	I dobët	Emër + vit lindjeje — lehtë i gjetshën
Kf#9mL!2xQp	I fortë	Kombinim i plotë, mbi 10 karaktere, rastësor
fjalëkalimi		

Më pas, mësuesi prezanton konceptin e autentikimit me dy faktorë (2FA), duke shpjeguar se ai bazohet në dy elemente sigurie: diçka që përdoruesi e di dhe diçka që ai zotëron. Përmes shembujve të thjeshtë, nxënësit kuptojnë pse kjo masë e bën më të vështirë hyrjen e paautorizuar, edhe kur fjalëkalimi është zbuluar.

Në përfundim, nxënësit hartojnë rregullat e tyre personale për përdorimin e fjalëkalimeve të forta dhe reflektojnë mbi ndryshimet që mund të bëjnë në mënyrën si mbrojnë llogaritë e tyre.

***Produkti i mundshëm*:** Poster ose fletë personale me titull: "Rregullat e mia për një fjalëkalim të sigurt", e shoqëruar me një reflektim të shkurtër mbi ndryshimet që nxënësi do të zbatojë në praktikë.

RRJETET SOCIALE DHE PRIVATËSIA

✓ ***Çështjet kryesore që trajtohen:***

- Çfarë ndajmë dhe çfarë ruajmë private
- Cilësimet e privatësisë — si funksionojnë dhe si menaxhohen
- Pasojat afatgjata të ndarjes së informacionit
- Të drejtat digjitale të fëmijëve

Veprimtari: Do ta postoja? – Filtri i privatësisë

***Qëllimi i veprimtarisë*:** Nxënësit dallojnë llojet e informacionit që mund të ndahet dhe ato që duhet të mbeten private, duke reflektuar mbi pasojat që mund të sjellë publikimi i tyre në internet.

Përshkrimi i veprimtarisë: Veprimtaria nis me një ushtrim individual. Mësuesi u shpërndan nxënësve kartela me lloje të ndryshme informacioni, si emri i plotë, numri i telefonit, adresa e shtëpisë, emri i shkollës, fotografi personale, planifikimi i pushimeve, nota shkollore, mendime personale apo fotografi të ndryshme nga jeta e përditshme. Çdo nxënës i rendit kartelat në tre kategori:

- *Postoj lirisht*
- *Vetëm me miq*
- *Nuk postoj kurrë*

Më pas zhvillohet një diskutim i hapur në klasë, ku nxënësit krahasojnë zgjedhjet e tyre dhe argumentojnë arsyet. Mësuesi i ndihmon të kuptojnë se jo çdo informacion ka të njëjtin nivel ndjeshmërie dhe se vendimi për ta ndarë duhet të merret me kujdes. Në këtë fazë, ai prezanton edhe pyetje orientuese si:

- "*A do të isha i qetë nëse këtë postim do ta shihnin prindërit ose mësuesit?*"
- *"Si do të ndihesha nëse kjo përmbajtje do të mbetej online edhe pas disa vitesh?"*

Në vijim, mësuesi paraqet një rast të thjeshtë studimor, ku ndarja e pakujdesshme e një informacioni personal ka çuar në pasoja, si shqetësim, cenim të privatësisë ose shfrytëzim nga të tjerë. Kjo i ndihmon nxënësit të lidhin veprimtarinë me situata reale.

Në përfundim, nxënësit hartojnë disa rregulla personale për ndarjen e informacionit në internet, duke reflektuar mbi atë që duhet dhe nuk duhet të publikohet.

Produkti i mundshëm: Tri kategori të personalizuara të informacionit dhe një listë me rregullat personale të ndarjes së informacionit në internet.

Veprimtari: Hetues i privatësisë dhe cilësimet

Qëllimi i veprimtarisë: Nxënësit analizojnë profile të imagjinuara në rrjetet sociale, identifikojnë problemet e privatësisë dhe kuptojnë rëndësinë e menaxhimit të cilësimeve të privatësisë në mjedisin digjital.

Përshkrimi i veprimtarisë: Veprimtaria nis me analizën e një profili imagjinar të rrjetit social, të përgatitur paraprakisht nga mësuesi. Profili përmban elemente të ndryshme, si informacion personal, fotografi, komente, lista miqsh ose të dhëna të dukshme publikisht. Nën drejtimin e mësuesit, nxënësit vëzhgojnë profilin dhe diskutojnë:

- çfarë informacioni personal është i dukshëm;
- kush mund ta shohë atë;
- cilat elemente mund të përbëjnë rrezik për privatësinë;
- çfarë duhet ndryshuar për ta bërë profilin më të sigurt.

Më pas, mësuesi shpjegon në mënyrë të thjeshtë dhe vizuale disa nga cilësimet bazë të privatësisë në platformat online, si:

- kush mund të shohë postimet;
- kush mund të dërgojë kërkesa miqësie;
- kush mund ta gjejë profilin përmes kërkimit;
- si kufizohet dukshmëria e informacionit personal.

Në vijim, nxënësit ndahen në grupe dhe secili grup merr një profil imagjinar të ndryshëm për ta "audituar". Detyra e tyre është të identifikojnë problemet kryesore të privatësisë dhe të propozojnë ndryshime konkrete që do ta bënin profilin më të mbrojtur.

Pas analizës, grupet prezantojnë gjetjet e tyre para klasës dhe mësuesi përmbledh idetë kryesore, duke theksuar se privatësia në internet nuk mbrohet vetëm duke mos postuar, por edhe duke menaxhuar me kujdes cilësimet dhe informacionin që lëmë të dukshëm për të tjerët.

Produkti i mundshëm*:** Raport i shkurtër grupi me titull **"Auditimi i privatësisë***"**, ku përfshihen problemet e identifikuara dhe rekomandimet konkrete për mbrojtjen e profilit.

REAGIMI, RAPORTIMI DHE NDIHMA

Çështjet kryesore që trajtohen:

- Si dhe ku raportoj incidente kibernetike
- Kujt i drejtohem — harta e burimeve të ndihmës
- Përgatitja dhe prezantimi i fushatës ndërgjegjësuese

Veprimtari: Rruga e raportimit

***Qëllimi i veprimtarisë*:** Nxënësit kuptojnë dhe organizojnë hapat që duhen ndjekur për raportimin e incidenteve kibernetike, duke identifikuar personat dhe strukturat ku mund të drejtohen për ndihmë.

***Përshkrimi i veprimtarisë*:** Veprimtaria zhvillohet përmes punës në grup me skenarë të ndryshëm incidentesh, si raste të bullizmit kibernetik, marrje e një email-i phishing ose ndarje e paautorizuar e të dhënave personale. Çdo grup merr një skenar dhe ndërton një diagramë hap pas hapi, ku paraqet qartë:

- çfarë duhet bërë fillimisht;
- kujt duhet t'i drejtohet nxënësi;
- çfarë informacioni ose dëshmie duhet ruajtur;
- cilat veprime duhen shmangur.

Në vijim, grupet prezantojnë diagramin e tyre para klasës. Nxënësit dhe mësuesi diskutojnë mbi hapat e propozuar, identifikojnë nëse mungon ndonjë element dhe shqyrtojnë alternativa të mundshme. Mësuesi plotëson informacionin duke paraqitur edhe burimet kryesore të ndihmës, si mësuesi, prindi, psikologu i shkollës, linjat e ndihmës për fëmijë dhe institucionet përgjegjëse. Në përfundim, theksohet se raportimi në kohë është një hap i rëndësishëm për mbrojtjen e vetes dhe të të tjerëve në mjedisin digjital.

***Produkti i mundshëm*:** Diagramë e rrugës së raportimit për secilin skenar dhe një kartë e thjeshtë me kontaktet ose burimet ku nxënësi mund të kërkojë ndihmë.

Veprimtari: Kuizi i sigurisë kibernetike

Qëllimi i veprimtarisë: Nxënësit përforcojnë dhe vetëvlerësojnë njohuritë e fituara gjatë modulit përmes një kuizi formativ.

Përshkrimi i veprimtarisë: Mësuesi organizon një kuiz me pyetje që lidhen me temat kryesore të trajtuara në modul, si bullizmi kibernetik, mashtrimet elektronike, privatësia, raportimi dhe përdorimi i sigurt i teknologjisë. Pyetjet mund të jenë me alternativa, vërtetë/gabim, plotësim ose të mbështetura në skenarë të shkurtër.

Kuizi mund të zhvillohet me fletë pune ose përmes një platforme interaktive, në varësi të kushteve dhe mjeteve që ka në dispozicion mësuesi. Pas përfundimit të tij, zhvillohet një diskutim i shkurtër mbi pyetjet që rezultuan më të vështira, me qëllim sqarimin e keqkuptimeve dhe përforcimin e njohurive kryesore. Nxënësit ftohen të reflektojnë mbi rezultatet e tyre, duke identifikuar çfarë kanë kuptuar më mirë dhe cilat çështje kërkojnë ende më shumë vëmendje.

Produkti i mundshëm: Fletë kuizi e plotësuar dhe një reflektim individual mbi njohuritë e fituara dhe çështjet që duhen rishikuar.

Veprimtari: Përgatitja e fushatës ndërgjegjësuese

***Qëllimi i veprimtarisë*:** Nxënësit planifikojnë dhe organizojnë punën në grup për realizimin e produktit final të modulit.

***Përshkrimi i veprimtarisë*:** Veprimtaria nis me një diskutim të shkurtër, ku mësuesi rikujton qëllimin e produktit final dhe prezanton formatet e mundshme të fushatës ndërgjegjësuese, si poster, broshurë, skeç, video ose kuiz. Më pas, nxënësit ndahen në grupe dhe secili grup zgjedh formatin me të cilin dëshiron të punojë.

Në vijim, grupet planifikojnë punën e tyre, duke përcaktuar:

- mesazhin kryesor që duan të përcjellin;
- rolet e secilit anëtar të grupit;
- materialet që do të përdorin;
- hapat dhe afatet për realizimin e produktit.

Mësuesi ndjek procesin nga afër, jep orientime dhe ndihmon grupet të sqarojnë idetë, të organizojnë më mirë përmbajtjen dhe të përzgjedhin mënyrën më të përshtatshme për ta prezantuar atë para bashkëmoshatarëve.Në përfundim, secili grup paraqet shkurtimisht planin e vet të punës dhe draftin fillestar të produktit që synon të zhvillojë.

Produkti i mundshëm: Plan i detajuar i fushatës ndërgjegjësuese dhe drafti i parë i materialit që do të prezantohet.

8. PRODUKTI FINAL I MODULIT

Në përfundim të modulit, nxënësit realizojnë një produkt përfundimtar në grup, i cili demonstron në mënyrë të integruar njohuritë, aftësitë dhe qëndrimet e zhvilluara gjatë gjithë procesit mësimor. Produkti final synon të lidhë të nxënit me situata reale dhe të nxisë angazhimin aktiv të nxënësve në ndërgjegjësimin e bashkëmoshatarëve dhe të komunitetit shkollor për çështje që lidhen me sigurinë kibernetike, përdorimin e përgjegjshëm të internetit dhe mbrojtjen në mjedisin digjital.

Produkti final realizohet në formën e një fushate ndërgjegjësuese me temë, p.sh. “Unë lundroj i sigurt në internet”, ku nxënësit, të ndarë në grupe, përgatisin dhe prezantojnë materiale të ndryshme informuese dhe sensibilizuese për bashkëmoshatarët e tyre.

Produkti mund të marrë forma të ndryshme, si p.sh.:

- ***Poster ose infografikë*** me mesazhe të qarta për bullizmin kibernetik, mashtrimet elektronike, mbrojtjen e të dhënave personale ose përdorimin e sigurt të rrjeteve sociale;
- ***Broshurë ose fletëpalosje informuese*** me këshilla praktike për reagimin në situata të pasigurta online;
- ***Prezantim i shkurtër***, inskenim, video ose kuiz ndërgjegjësues, i ndërtuar mbi skenarë dhe situata të trajtuara gjatë modulit.

Gjatë realizimit të produktit final, nxënësit planifikojnë punën në grup, ndajnë rolet dhe përgjegjësitë, përzgjedhin mesazhet kryesore dhe i paraqesin ato në mënyrë të kuptueshme, tërheqëse dhe të përshtatshme për audiencën.

Produktet mund të prezantohen në klasë ose në një aktivitet të përbashkët në nivel shkolle, ku nxënësit shpjegojnë punën e tyre, ndajnë mesazhet kryesore dhe ndërveprojnë me bashkëmoshatarët përmes pyetjeve, diskutimeve ose aktiviteteve ndërgjegjësuese. Produktet mund të ekspozohen në mjediset e shkollës ose të publikohen në hapësirat informuese të saj, me qëllim rritjen e ndërgjegjësimit të komunitetit shkollor mbi sigurinë kibernetike dhe përdorimin e përgjegjshëm të teknologjisë.

Shënim: Moduli që zhvillohet në kuadër të kurrikulës me bazë shkolle vlerësohet vetëm mbi bazën e kryerjes së modulit (moduli nuk vlerësohet me notë).

9. SHTOJCA

Shtojca 1: Skenarë shtesë — Bullizmi kibernetik

Nr.	Skenari	Pyetjet për diskutim
1	Besi publikon në rrjet komente fyese dhe përçmuese ndaj disa shokëve të klasës. Pas pak, edhe nxënës të tjerë bashkohen me komente negative dhe situata përshkallëzohet.	Kush është autori kryesor i kësaj situate? Si ndikon përfshirja e nxënësve të tjerë në përshkallëzimin e saj? Çfarë duhet të bëjnë nxënësit që janë etiketuar ose përmendur? Çfarë përgjegjësie kanë ata që kanë komentuar ose kanë reaguar negativisht?
2	Mira merr çdo natë, pas mesnatës, mesazhe kërcënuese nga një numër i panjohur. Personi i shkruan se e di ku banon dhe i kërkon të mos i tregojë askujt. Mira ndihet e frikësuar dhe heziton të flasë.	Çfarë rreziku paraqet kjo situatë për Mirën? Pse mund të ketë frikë ajo ta tregojë këtë? Cilat janë shenjat që tregojnë se situata është serioze? Çfarë duhet të bëjë menjëherë Mira dhe kujt duhet t'i drejtohet?

3	Arbi dhe Kleidi kanë pasur një konflikt personal. Pas kësaj, Kleidi krijon një llogari të rreme me emrin dhe të dhënat e Arbit dhe publikon përmbajtje të papërshtatshme, duke bërë që shokët të besojnë se llogaria është e Arbit.	Si quhet kjo formë e bullizmit kibernetik? Si ndikon kjo situatë në imazhin dhe reputacionin e Arbit? Çfarë hapash duhet të ndërmarrë ai për të treguar se llogaria nuk është e tij? Ku duhet të drejtohet për ndihmë dhe raportim?
4	Në grupin e klasës në WhatsApp, disa nxënës fillojnë të bëjnë shaka për mënyrën si vishet një nxënëse. Me kalimin e kohës, komentet bëhen gjithnjë e më fyese dhe ajo vendos të dalë nga grupi.	Në cilin moment situata kalon nga shaka në bullizëm kibernetik? Si mund të ndikojë kjo te nxënësja që është vënë në shënjestër? Cili është roli i administratorit të grupit në këtë rast? Çfarë duhet të bëjnë anëtarët e tjerë të grupit për ta ndalur situatën?
5	Një nxënëse fotografon fshehurazi shoqen e saj gjatë orës së edukimit fizik dhe e shpërndan fotografinë në grupin e klasës, duke e shoqëruar me komente tallëse.	Cilat të drejta të nxënëses janë cenuar në këtë rast? Pse shpërndarja e një fotografie pa leje është veprim i gabuar? Çfarë pasojash emocionale, sociale ose edhe ligjore mund të ketë kjo situatë? Si duhet të reagojë viktima dhe si duhet të veprojnë nxënësit që e shohin fotografinë?

Shtojca 2: Skenarë shtesë — Phishing

Nr.	**Skenari**	**Shenjat paralajmëruese**
1	Një nxënës merr një email me përmbajtjen: “Llogaria jote Roblox do të fshihet! Kliko këtu brenda 24 orësh dhe fut emrin dhe fjalëkalimin për ta ruajtur.” Dërguesi shfaqet si: *noreply@roblox-security-center.net*	Adresë dërguesi e dyshimtë dhe jozyrtare; përdorim i gjuhës urgjente dhe kërcënuese; vendosje afati kohor për të krijuar presion; kërkesë për emër përdoruesi dhe fjalëkalim, të cilat platformat zyrtare nuk i kërkojnë në këtë formë.
2	Një nxënës merr një mesazh SMS me përmbajtjen: “Mami ka probleme, na është prishur telefoni. Jam te fqinji. Dërgomë 50 euro në këtë numër karte dhe të shpjegoj gjithçka.”	Kërkesë e menjëhershme për para; përdorim i urgjencës për të nxitur reagim të shpejtë; imitim i një personi të besuar; mungesë verifikimi të identitetit; mesazhi vjen nga një numër i panjohur.
3	Në ekranin e kompjuterit shfaqet një dritare paralajmëruese me tekstin: “VIRUS I GJETUR! Sistemi juaj është infektuar me 13	Dritare paralajmëruese e pakërkuar; gjuhë alarmuese dhe frikësuese; pretendim i ekzagjeruar për infektim; kërkesë për veprim të menjëhershëm; ofertë e

	viruse. Kliko TANI për ta pastruar falas!", e shoqëruar me alarm zanor.	pakërkuar për "zgjidhje falas"; përdorim i manipulimit për të krijuar panik dhe presion psikologjik.
4	Një nxënës merr në Instagram një mesazh nga një llogari që duket si e shokut të tij, por është krijuar së fundi. Mesazhi thotë: "Shiko foton tënde këtu!" dhe përmban një lidhje të shkurtuar.	Llogari e dyshimtë ose e sapokrijuar; mesazh i shkurtër dhe jopersonal; lidhje e shkurtuar që fsheh adresën reale; përmbajtje që synon të zgjojë kureshtje ose shqetësim; mundësi për imitim të një personi të njohur.
5	Një nxënës hap një faqe interneti që duket identike me faqen e bankës, por adresa është: *www.bankë-kombëtare-login.com/secure*. Faqja kërkon numrin e kartës dhe kodin CVV.	Adresë interneti jozyrtare dhe e dyshimtë; përpjekje për të imituar faqen origjinale të bankës; kërkesë për të dhëna shumë sensitive, si numri i kartës dhe CVV; përdorim i një faqeje të kopjuar vizualisht për të krijuar besim të rremë; mungesë e elementeve të besueshme të sigurisë.

Shtojca 3: Fjalori i termave kryesorë

- ***Bullizmi kibernetik*** — ngacmim, frikësim ose dëmtim i dikujt nëpërmjet internetit, telefonit ose mjeteve digjitale, me qëllim dhe në mënyrë të përsëritur.
- ***Phishing*** — tentativë mashtrimi ku krimineli digjital paraqitet si dikush i besuar (bankë, platformë, shok) për të vjedhur informacion personal ose para.
- ***Smishing*** — phishing nëpërmjet SMS — mesazhe teksti mashtruese që imitojnë institucione ose persona të njohur.
- ***Vishing*** — phishing nëpërmjet telefonit — thirrje mashtruese ku dikush pretendon të jetë bankë, polici ose institucion tjetër.
- ***Gjurma digjitale*** — tërësia e informacionit që lëmë pas çdo herë që përdorim internetin: klikime, kërkime, postime, komente, llogari të hapura.
- ***Identiteti online*** — mënyra si paraqitemi dhe perceptohemi në internet — profili, fotot, komentet dhe sjelljet tona digjitale formojnë këtë identitet.
- ***Fjalëkalim i fortë*** — kombinim i gjatë (12+ karaktere) i shkronjave të mëdha e të vogla, numrave dhe simboleve, i ndryshëm për çdo llogari.
- ***2FA (Autentikimi me dy faktorë***) — sistem sigurie ku për të hyrë në llogari kërkohen dy prova identiteti: zakonisht fjalëkalimi dhe kodi i dërguar në telefon.
- ***Vëzhguesi*** (Bystander) — personi që është dëshmitar i bullizmit kibernetik pa qenë as viktimë as autor. Vendimi i tij për të ndërhyrë ose jo ndikon drejtpërdrejt në dinamikën e situatës.
- ***Privatësia digjitale*** — e drejta dhe mundësia për të kontrolluar çfarë informacioni ndajmë online, me kë dhe si përdoret ai informacion.
- ***Malware*** — program kompjuterik i dëmshëm që instalohet fshehurazi dhe mund të vjedhë të dhëna, të bllokojë sistemin ose të dëmtojë pajisjen.

- ***Raportimi online*** — mundësia e ofruar nga platformat digjitale për të njoftuar mbi përmbajtje ose llogari që shkelin rregullat e komunitetit.
- ***Qytetaria digjitale*** — tërësia e të drejtave, detyrimeve dhe sjelljeve etike që priten nga çdo person që përdor teknologjinë dhe internetin.
- ***HTTPS*** — protokoll i sigurt komunikimi në internet — faqet me HTTPS enkriptojnë të dhënat tuaja. Mungesa e HTTPS mund të jetë shenjë rreziku.
- ***Enkriptimi*** — proces i kodimit të informacionit në mënyrë që vetëm personi i autorizuar mund ta lexojë. Fjalëkalimet dhe mesazhet e siguruara përdorin enkriptim.
- ***Algoritmi i rrjetit social*** — sistemi i automatizuar i platformës që vendos çfarë shikojmë në feed, bazuar mbi klikime, shikime dhe reagime të kaluara.
- ***Krimi kibernetik*** — veprimtari kriminale e kryer nëpërmjet internetit ose mjeteve digjitale — phishing, hakimi dhe shantazhi online janë shembuj tipikë.